



(12) **EUROPEAN PATENT APPLICATION**
published in accordance with Art. 153(4) EPC

(43) Date of publication:
19.09.2012 Bulletin 2012/38

(21) Application number: **10828363.1**

(22) Date of filing: **05.11.2010**

(51) Int Cl.:
G07G 1/12 (2006.01) **G06F 21/20** (2006.01)
G06Q 10/00 (2012.01) **G06Q 20/00** (2012.01)
G09C 1/00 (2006.01) **H04L 9/32** (2006.01)

(86) International application number:
PCT/JP2010/069754

(87) International publication number:
WO 2011/055804 (12.05.2011 Gazette 2011/19)

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priority: **09.11.2009 JP 2009256218**

(71) Applicant: **NEC Infrontia Corporation**
Kawasaki-shi
Kanagawa 213-8511 (JP)

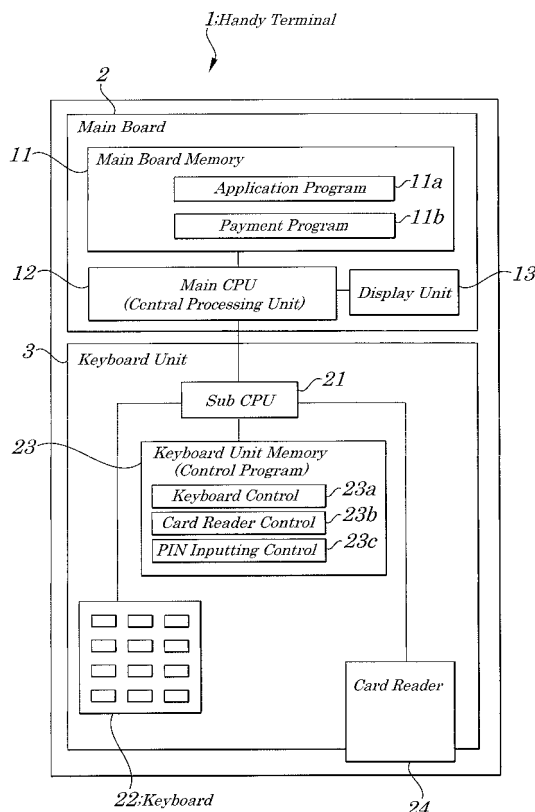
(72) Inventor: **KOMIYAMA Tsuyoshi**
Kawasaki-shi
Kanagawa 213-8511 (JP)

(74) Representative: **Vossius & Partner**
Siebertstrasse 4
81675 München (DE)

(54) **HANDY TERMINAL AND PAYMENT METHOD USED FOR THE HANDY TERMINAL**

(57) There is provided a handy terminal in which inputting of an application program and of a PIN is executed and a keyboard and a display device are commonly used thus security is secured with a simple system. A card reader control program 23b in the keyboard unit memory 23 detects an insertion state of a credit card and notifies a detected key cord from the keyboard control program 23a to a payment program on the main board 2. A main CPU 12 calculates a program hash value provided to the payment program and a program hash value at the time of execution of a payment program 11b and encrypts and decrypts these hash values using a secret key, encrypted key, and public key so that these hash values are not stolen. The main CPU 12 compares the program hash value provided to the payment program 11b with the program hash value to be used at the time of the execution of the payment program 11b.

FIG. 1



Description

TECHNICAL FIELD

[0001] The present invention relates to a handy terminal and a payment method to be used in the handy terminal and more particularly to the handy terminal and the payment method suitably used in a portable information terminal having a payment capability to make a settlement for a credit card.

BACKGROUND TECHNOLOGY

[0002] For a handy terminal to perform a process by inputting a PIN (Personal Identification Number) of a credit card, PCIDSS (Payment Card Industry Data Security Standard) being an international uniform standard for security of a payment card is regulated. According to the international uniform standard, by providing a handy terminal with a keyboard for dedicated use for inputting of a PIN and a display device, stealing of a PIN code can be prevented. That is, when a PIN of a credit card is inputted, in addition to a keyboard to be used in the application program, by providing a keyboard for dedicated use, inputting of the PIN is executed. Moreover, a display device for an application program is separated from a display device to be used in inputting of the PIN. Thus, in the execution of inputting of a PIN and of the application program by operating the keyboard and display device in a separated manner, the PIN code can be also prevented from being stolen.

[0003] As a related technology of this kind, there is an order payment system disclosed in Patent Reference 1. By using the order payment system, for example, at a restaurant and a like, by cooperating a POS (Point of Sales) with a handy terminal at a seat, without operations at the POS, a payment process of a credit card while at the seat can be performed.

[0004] In the payment device disclosed in Patent Reference 2, an IC card and PDA (Personal Digital Assistance) device are so constructed to be operated in a co-operated manner and customer information A is, in advance, registered with a payment server. When a PIN inputted by a customer into the PDA is aligned with a PIN of the IC card, customer information B is transmitted to from the PDA to the payment server. Then, when the customer information B transmitted from the PDA to the payment server is aligned with the customer information A registered with the payment server, an instruction for payment of the IC card is provided from the payment server to the PDA. By these operations, the prevention of stealing customer's information and the settlement of a credit card can be simultaneously realized.

[0005] Moreover, in a data processing device disclosed in Patent Reference 3, in a multi CPU system made up of a main CPU board and a sub CPU board, only when the sub CPU board performs authentication by using a certified secret key and a running program,

the process of payment is performed by the main CPU board. Thus, by separating the sub CPU board for certification from the main CPU board for execution of the payment processing, the settlement process of a card can be performed while preventing the steal of customer information.

RELATED ART DOCUMENT

10 Related Art Patent References

[0006]

Related Art Patent Reference 1: Japanese Patent Application Laid-open No. 2002-133533.

Related Art Patent Reference 2: Japanese Patent Application Laid-Open No. 2005-182315.

Related Art Patent Reference 3: Japanese Patent Application Laid-Open No. 2006-178544.

SUMMARY OF INVENTION

Problems to be solved by the Invention

25 **[0007]** However, in the case of the technologies disclosed in the above Related Art Patent References have the following problems: That is, if one portable information terminal is used as a dedicated device for inputting a PIN, in addition to this device, another portable information terminal for an application program must be prepared and, as a result, two portable information terminals must be also prepared, which causes portability to be lost. Moreover, if two keyboards for an application program and for inputting a PIN, two keyboards and two display device have to be mounted in one portable information terminal, thus inevitably causing an increase in manufacturing costs and further, its applications are also limited, which becomes a factor distributing the development of products of the portable information terminal.

30 **[0008]** Then, if the keyboard to be used in an application program and display device can be commonly used in the putting of a PIN, one portable information terminal can be made small-sized. In other words, an application program and a program for inputting a PIN can share the keyboard and display device, which enables a platform for software and hardware being an environment to be commonly used, as a result, it is made possible to miniaturize a device for a portable information terminal and to achieve effectively device development of products in the portable information terminal. This enables improvement of portability of a portable information terminal, simplification of manufacturing design and manufacturing costs, reduction of product costs, and improvement of convenience of a portable information terminal for users. However, there is a problem that, by commonly using a keyboard for an application program and a program for inputting a PIN and a display device, when a spurious screen program is installed, a pseudo screen for inputting

a PIN, which causes a PIN cord to be stolen.

[0009] Moreover, the order settlement system disclosed in the Patent Reference 1 is designed for performing the settlement by cooperation between the handy terminal for dedicated use of the settlement and a POS and, as a result, the handy terminal system cannot solely performs the settlement processes. This handy terminal is used not for development of an application program but for only payment process for a credit card. Therefore, by using this technology, it is impossible to realize a handy terminal capable of using commonly a keyboard for the application program and a program for inputting a PIN cord and a display device.

[0010] In the payment system disclosed in the Patent Reference 2, the PDA is designed to perform the settlement process while preventing stealing of a PIN cod by cooperation with the settlement server and, therefore, the settlement process system becomes complicated accordingly. In addition, the PDA is not provided with a function of performing the settlement process while solely preventing stealing of a PIN and, therefore, as in the case of the Patent Reference 1, it is impossible to achieve the technology to commonly use a keyboard for an application program and a program for inputting a PIN, and display device.

[0011] Also, in the data processing device disclosed in the Patent Reference 3, it is made possible to perform settlement processing while preventing stealing of a PIN code by cooperation between the main CPU board and the sub CPU board, however, the payment processing system becomes complicated. Therefore, by using the technology, it is impossible to expand the technology so that the main CPU board or sub CPU board can solely prevent the stealing of a PIN code while performing the settlement processing at the same time.

[0012] In view of the above, an object of the present invention is to provide a handy terminal and a payment method to be used in the handy terminal to have a settlement function of ensuring security with a simple system even when a keyboard for inputting of an application program and inputting of a PIN and a display device are commonly used.

Means for Solving the Problems

[0013] In order to solve the above problems, according to a first feature configuration of the present invention, there is provided a handy terminal having a payment capability in which inputting of an application program and inputting of a PIN of a credit card which is controlled by a payment program is able to be processed by a common keyboard, the handy terminal including a payment program legitimacy judging unit to judge whether or not the payment program, inputting of which is required, is legitimately released when an inserted state of a credit card is detected, by using a program hash value of the payment program.

[0014] According to a second feature configuration of

the present invention, there is provided a payment method to be used in a handy terminal in which, inputting of an application program and inputting of a PIN of a credit card which is controlled by a payment program is able to be processed by a common keyboard, the payment method including a first step of detecting a state of insertion of the credit card and a second step of judging, when a state of insertion of the credit card in the first step, using a program hash value of the payment program, whether or not the payment program, inputting of which is requested, is legitimately released.

EFFECTS OF INVENTION

[0015] According to the present invention, even when a keyboard for an application program, a program for inputting a PIN, and a display device are commonly used by making, in advance, a designated program certification to conform legitimacy of a payment program, stealing of the PIN code of a credit card can be prevented. When a state of inserting of a credit card is detected, notification of the inputting of the PIN is made only to the certified program. Moreover, in a state where the credit card has been extracted, an existing application program can be operated as a general-use keyboard, which enables the versatility of a designated level to be obtained.

BRIEF DESCRIPTION OF DRAWINGS

[0016]

Figure 1 is a block diagram showing configurations of a handy terminal according to one embodiment of the present invention.

Figure 2 is a flow chart showing a flow of operations of the handy terminal of Fig. 1.

Figure 3 is a flow chart showing a flow of the preparation for installing a module in Steps S1 and S2 of Fig. 2.

Figure 4 is a flow chart showing a flow of a certification process of a payment program 11b in the Step S6 of Fig. 2.

BEST MODE OF CARRYING OUT THE INVENTION

[0017] A handy terminal is realized which includes a detecting means to detect a state of inserting and extracting of a credit card, a hash value calculating means to calculate a first program hash value provided to a payment program and a second hash program used at time of the execution of the program, which are used to detect alteration of the payment program, an encryption means to encrypt the first program hash value and the second program hash value calculated by the hash value calculating means, a decryption means to decrypt, by using a first key, the first program hash value and the second program hash value encrypted by the encryption means, a hash value comparing means to compare the first pro-

gram hash value with the second program hash value to judge whether or not the payment program is legitimately released, and a key cord notification controlling means to control the notification of a key cord based on an inserting and extracting state of the above credit card detected by the detecting means when results obtained by the hash value comparing means are aligned with one another.

[0018] When the payment program legitimacy judging means judges that the payment program is legitimate, the execution of inputting of a PIN code of the above credit card is enabled and, when the payment program legitimacy judging means judges that the payment program is illegitimate, the notification of a key cord is rejected and the execution of inputting of the PIN code is disabled. When the hash value comparing means judges that the first program hash value is aligned with the second program hash value, the above key cord notification controlling mean enables the execution of inputting the PIN code of a credit card and when the hash value comparing means judges that the first program hash value is not aligned with the second program hash value, the key cord notification controlling means rejects the notification of the key cord and disables the execution of inputting the PIN code.

[0019] The handy terminal also has a coupling means to couple an encrypted first program hash value to the payment program which installs the encrypted first program hash value and the payment program as a coupled module in a main board memory. Moreover, the above first key is an encrypted key produced by using a secret key and a random number and the second key is the encrypted key and public key and the first program hash key and second program hash key are encrypted by using at least one of the secret key and encrypted key and the encrypted first program hash value and second hash value are decrypted by using the public key or the encrypted key.

FIRST EMBODIMENT

[0020] Hereinafter, by referring to drawings, embodiments of the handy terminal of a payment capability providing type of the present invention are described in detail. Figure 1 is a block diagram showing configurations of a handy terminal of the first embodiment of the present invention. As shown in Fig. 1, the handy terminal 1 is made up of a main board 2 and a keyboard unit 3. The main board 2 includes a main board memory 11 to execute programs (application program 11a and payment program 11b) on the main board 2, a main CPU (Central Processing Unit) 12 to perform processing on entire operations of the handy terminal 1, and a display unit 13 to display contents of the application program 11a and payment program 11b and/or contents inputted from outside.

[0021] The keyboard unit 3 includes a sub CPU 21 to control various kinds of programs mounted on the keyboard unit 3, a keyboard 22 serving as a user interface

to input data for various operations, a keyboard unit memory 23 to execute various control programs (keyboard control program 23a, card reader control program 23b, and PIN inputting control program 23c) installed in the keyboard unit 3, and a card reader 24 to read information stored in a credit card.

[0022] Figure 2 is a flow chart showing a flow of operations of the handy terminal shown in Fig. 1. Figure 3 is also a flow chart showing a flow of operations including install module preparation and registration of devices in Step S1 and Step S2 in Fig. 2. Figure 4 is a flow chart showing a flow of operations of certifying the payment program in Step S6 of Fig. 2. By referring to these drawings, contents of processing for payment method to be used in the handy terminal of the embodiment.

[0023] The flows of operations of the main board 2 and the keyboard unit 3 are shown in Fig. 2.

That is, as shown in Fig. 2, a module to be installed in the handy terminal 1 is prepared (Step S1) and the module is registered with a device of the handy terminal 1 (Step S2). When the registration of the module with the device of the handy terminal (install operation) is completed (Step S2), the processing of works at an ordinary operation is started (Step S3). By this, the keyboard unit 3 is operated as a generally used keyboard and inputting operation of the keyboard is performed by a user. Here, when the keyboard unit 3 detects the keyboard inputting and then informs the main board 2 of the inputting (Step S4), by the application program 11a of the main board memory 11, a keyboard is obtained from the keyboard inputting information of the keyboard unit 3 (Step S5).

[0024] Moreover, the keyboard unit 3 of the handy terminal 1 can also perform the inputting of the PIN code. At this point of time, in order to prevent the PIN code from being stolen by a malicious program, a certification process of the payment program 11b installed in the main board memory 11 on the main board 2 is performed (Step S6). The certification of the payment program 11b is performed every time the payment program is booted (that is, an EXE file is executed).

[0025] After the certification of the payment program 11b to be performed at Step 6 is completed, the insertion is detected by the card reader control program 23b installed in the keyboard unit memory 23 on the keyboard unit 3 (Step S7). From the result of comparison between a first hash value provided to the payment program 11b and a second hash value calculated at the time of execution of the payment program 11b, the payment program is judged to be legitimate, the inputting of a key code into the keyboard 22 is detected (Step S8). The detected keyboard is notified from the keyboard control program 23a installed in the keyboard unit 3 to the main board 2. By this operation, the payment program 11b stored in the main board memory 11 on the main board 2 obtains a key code (Step S9). Moreover, when, by the result of the comparison of the hash values, the program is judged to be illegitimate, the keyboard unit 3 does not notify the inputting of a keyboard to the main board 2.

[0026] When the payment program 11b obtains a key code at Step S9, while a PIN code of a credit card is being inputted (Step 10), though the keyboard unit 3 continues the notification of the inputting of a key code to the payment program 11b (Step S8), the key cord to be notified is "*"code". Finally, when the extraction of a credit card is detected (Step S11), all the results from comparisons of hash values are cleared and the program returns back to the process by the general-use keyboard performed at Steps S4 and S5.

[0027] In the processes of the preparation of the install module and the registration of the device, in order to prevent the program hash value from being stolen, a program producer must prepare a public key to be distributed to general persons which is an asymmetric key in which a key to be used in encryption is separated from a key to be used in decryption (Step S21) and further prepares a secret key which its owner himself or herself knows (Step S22). Next, the payment program 11b stored in the main board memory 11 in the main board 2 is prepared (Step S23) and by using a developed PC (Personal Computer), a hash value provided by the main CPU 12 to the payment program 11b is calculated (Step S24). Moreover, the hash value is a value calculated according to a calculation method by which a random number of fixed length is produced from given data in the payment program 11b and, by utilizing the hash value, retrieving time of data can be shortened.

[0028] Next, for the prevention from stealing of the hash value, by using a secret key prepared by Step S22, the hash value calculated at Step S24 is encrypted (Step S25). Then, the encrypted hash value is coupled to the payment program 11b (Step S26) and the coupled module (i.e., encrypted hash value and payment program 11b) is installed in the main board memory 11 of the main board 2 in the handy terminal 1 (Step S27).

[0029] The application program 11a to perform a process of work is also installed in the main board memory 11 on the main board 2 (Step S28). Moreover, the public key prepared at Step 21 in order to decrypt a hash value is installed in the keyboard unit memory 23 on the keyboard unit 3 (Step S29).

[0030] In the process of authenticating the payment program 11b at Step S6 in Fig. 2, as shown in Fig. 4, the hash value coupled at Step S26 in Fig. 3 is first separated from a coupled (encrypted) module to the payment program (Step S31) and the payment program 11b is left on the main board (Step S32) and an encrypted hash value is transferred to the keyboard unit 3 (Step S33). Then, the sub CPU 21 in the keyboard unit 3 decrypts the hash value by using the registered public key (Step S34) to make the hash value be unencrypted (Step S35).

[0031] On the other hand, on the main board 2 side, the hash value is calculated by the main CPU 12 to be used at the time of execution of the payment program 11b left at Step 32 (Step S36). In order to prevent wire-tapping between the main board 2 and the keyboard 22 in the keyboard unit 3, an encrypted key is produced by

using a random number on the keyboard unit 3 side (Step S37) and the encrypted key is transferred to the main board 2. Then, on the main board 2 side, by using the encrypted key received from the keyboard unit 3, the hash value calculated by the main CPU 12 at Step S36 is encrypted (Step S38) and encrypted hash value is transferred to the keyboard unit 3 (Step S39).

[0032] By this operations, the keyboard unit 3 receives the encrypted hash value from the main board 2 (Step S40), and by using the encrypted key produced at Step S37, the encrypted hash value is decrypted and a resulting unencrypted hash value is taken out (Step S41). Further, the developed PC compares the first hash value provided to the payment program 11b calculated by the main CPU 12 at Step S24 in Fig. 3 with the second hash value calculated by the main CPU 12 at Step S36 in Fig. 4 at the time of the execution of the payment program (Step S42). If the comparison result shows that the first hash value is aligned with the second hash value, the payment program 11b is determined to be certified and the certification result is stored in the keyboard unit memory 23 on the keyboard unit 3 side (Step S43).

[0033] Moreover, the reason for encryption of a hash value is shown as the following reason (1) and (2):

(1) By confirming whether or not a logic for encryption of a hash value is legitimate, it can be judged whether the process on the main board 2 is legitimate.

(2) A serial interface portion between the main board 2 and the keyboard unit 3 is always monitored and, in order to prevent a hash value from being stolen and to prevent the hash value from being flown out, a hash value is encrypted by changing an encrypted key using a random number at every time of monitoring.

[0034] As described above, the handy terminal of the present invention is provided with a payment program legitimacy judging means to judge, when the insertion of a credit card is detected, whether the payment program demanded for inputting is released legitimately, by using the hash value of the payment program. When the payment program legitimacy judging means judges that the payment program is legitimate, a key cord is notified thus enabling the inputting of a PIN, while the payment program legitimacy judging means judges that the payment program is illegitimate, the notification of the key cord is denied thus disabling the inputting of the PIN. This enables the PIN code to be prevented from being read by a malicious third person.

[0035] The handy terminal of the present invention is made up of a detecting means to detect an insertion and extraction state of a credit card, a key cord notification control means to control the key code notification while a credit card is being inserted or extracted, a hash value calculating means to calculate a program hash value to detect the alteration of the payment program, an encryption and decryption means to encrypt or decrypt a pro-

gram hash value using a secret key and encrypted key possessed by a program producer, a coupling means to couple an encrypted hash value to a payment program, and a hash value comparing means to compare a hash value provided to the program with the hash value obtained by calculating at the time of execution of a program.

[0036] The detection for detecting an insertion and extraction state of a credit card is realized by detecting the insertion of a credit card by the card reader control program 23b installed in the keyboard unit memory 23. Moreover, the key cord notification control for controlling the key cord notification in a state where the credit card is being inserted or extracted is realized by notification of a detected key cord from the keyboard control program 23a in the keyboard unit 3 to the payment program 11b of the main board 2.

[0037] The hash value calculation to calculate a program hash value is realized by detecting the alteration of the payment program by calculating, using the main CPU 12, a hash value provided by the payment program 11b or the hash value obtained at the execution of the payment program 11b. Encryption and decryption of the program hash value by using a secret key, encrypted key, and public key possessed by a program producer's to prevent a program hash value from being stolen is achieved, by operations of the main CPU 12, and sub CPU 21, of encrypting and decrypting a hash value using the secret key, encrypted key, and public key.

[0038] The coupling of the encrypted hash value to the payment program is realized by coupling the encrypted hash value to the payment program to form a module and by installing the module in the main board memory 11 on the main board 2. Moreover, the hash value comparison to compare the hash value provided to a program with the hash value obtained by calculation at the time of execution of the program is realized by calculating, using the main CPU 12, a first hash value provided to the payment program 11b and the second hash value obtained at the execution of the payment program 11b and by comparing these two values.

[0039] Thus, according to the present embodiment, the handy terminal, even when the inputting of an application program and of the PIN code is performed by a common keyboard 22, prior to operations of the inputting of a PIN code, judges whether the payment program is legitimately released. At this time, if the payment program, the inputting of which is required, is legitimate, the key cord is notified and a Pin code can be inputted and if the payment program, the inputting of which is required, is illegitimate, the key cord is not notified, which, as a result, enables the PIN code to be prevented from being stolen.

[0040] Thus, the embodiment is described by referring to the drawings and it is apparent that the present invention is not limited to the above embodiments and may be changed and modified without departing from the scope and spirit of the present invention. For example, the

handy terminal by which the inputting of application programs and the PIN code can be performed by a common keyboard is not limited to the payment process of a credit card and, when the handy terminal is used for electronic money, illegitimate use of the electronic money by a third person can be prevented.

[0041] The present invention claims the priority based on Japanese Patent Application laid-open No. 2009-256218, the entire contents of which are incorporated herein by reference in its entirety.

INDUSTRIAL APPLICABILITY

[0042] The handy terminal of the present invention, by alternately using solely the application program and PIN inputting, stealing of the PIN code can be prevented, without cooperation with a host processor such as a POS, the handy terminal can be effectively used at a retail store and/or a selling area and the like.

EXPLANATION OF LETTERS AND NUMERALS

[0043]

- 1: Handy terminal,
- 2: Main board,
- 3: Keyboard unit,
- 11: Main board memory,
- 11a: application program,
- 11b: Payment program (hash value calculating means),
- 12: Main CPU (payment program legitimacy judging means, hash value calculating means, encryption means, coupling means),
- 13: Display unit,
- 21: Sub CPU (decryption means, hash value comparison means),
- 22: Keyboard,
- 23: Keyboard unit memory (key code notification control means),
- 23a: Keyboard control program (detecting means),
- 23b: card reader control program,
- 23c: PIN inputting control program,
- 24: Card reader.

Claims

1. A handy terminal having a payment capability in which inputting of an application program and inputting of a PIN of a credit card which is controlled by a payment program is able to be processed by a common keyboard, the handy terminal **characterized by** comprising:

a payment program legitimacy judging means to judge whether or not the payment program, inputting of which is required is, legiti-

mately released when an inserted state of a credit card is detected, by using a program hash value of the payment program.

2. A handy terminal having a payment capability the inputting of an application program and inputting of a PIN of a credit card which is controlled by the payment program is able to be processed by a common keyboard, the handy terminal **characterized by** comprising:

a detecting means to detect a state of insertion and extraction of the credit card;

a hash value calculating means to calculate a first program hash value provided to the payment program and a second program hash value to be used at a time of execution of a program; an encryption means to encrypt, by using a first key, a first program hash value and a second program hash value obtained by calculation of the hash value calculating means;

a decryption means to decrypt, by using a second key, the first program hash value and second program hash value encrypted by the encryption means;

a hash value comparison means to compare the first program hash value and the second program hash value decrypted by the decryption means to judge whether or not the payment program is legitimately released; and

a key cord notification control means to control notification of a key cord based on an insertion and extraction state of the credit card detected by the detecting means when results from the comparison by the hash value comparison means are aligned with each other;

3. The handy terminal according to Claim 1, **characterized in that** the payment program legitimacy judging means, when judging that the payment program is legitimate, enables the execution of inputting of a PIN code of the credit card, and when judging that the payment program is illegitimate, denies the notification of a key cord and disables the execution of inputting of the PIN code.

4. The handy terminal according to Claim 2, **characterized in that**, when the hash value comparison means judges that the first program hash value is aligned with the second program hash value, the key cord notification control means enables the inputting of the PIN cord of a credit card to be executed and when the hash value comparison means judges that the first program hash value is not aligned with the second program hash value, the key code notification control means denies the notification of a key cord and disables the execution of inputting of a PIN code.

5. The handy terminal according to Claim 2 or 4, **characterized by** further comprising a coupling means to couple the encrypted first program hash value to the payment program, in which the coupling means installs a module obtained by coupling the encrypted first program hash value to the payment program into the main board memory.

6. The handy terminal according to Claim 2, 4, or 5, **characterized in that** the first key is an encryption key produced by using a secret key and a random number and the second key is the encryption key and public key and the first program hash value and the second program hash value are produced by encryption by using, at least one of the first program hash value and the encryption key, and the encrypted first program hash value and the second program hash value are decrypted by using the public key or the encrypted key.

7. A payment method to be used in a handy terminal in which, inputting of an application program and inputting of a PIN of a credit card which is controlled by a payment program is able to be processed by a common keyboard, the payment method **characterized by** comprising:

a first step of detecting a state of insertion of the credit card; and

a second step of judging, when a state of insertion of the credit card in the first step is detected, using a program hash value of the payment program, whether or not the payment program, inputting of which is requested, is legitimately released.

8. A payment method to be used in a handy terminal in which, inputting of an application program and inputting of a PIN of a credit card which is controlled by a payment program is able to be processed by a common keyboard, the payment method **characterized by** comprising:

a first step of detecting an insertion and extraction state of a credit card;

a second step of calculating, in order to detect alteration of the payment program, a first program hash value provided by the payment program and the second program hash value to be used at a time of execution of a program;

a third step of encrypting, by using a first key, the first program hash value and the second program hash value calculated in the second step; a fourth step of decrypting, by using the second key, the first program hash value encrypted in the third step;

a fifth step of comparing the first program hash value decrypted by the fourth step with the sec-

ond program hash value to judge whether the payment program is legitimately released; and a sixth step of controlling the notification of a keyboard based on an insertion and extraction of the credit card detected in the first step when the comparison results are aligned with each other in the fifth step; 5

9. The payment method according to Claim 7, **characterized in that**, when the payment program is judged as a legitimate one, the execution of inputting of a PIN code of the credit card is enabled and when the payment program is judged as an illegitimate one, the notification of a key cord is denied and the execution of the inputting of the PIN code is disabled. 10 15
10. The payment method according to Claim 8, **characterized in that**, when the first program hash value judged to be aligned with the second program hash value in the fifth step and the execution of the PIN code of the credit card is enabled in the sixth step and the first program hash value is judged not to be aligned with the second program hash value, the notification of a key cord is denied in the sixth step and the execution of the inputting of a PIN code is disabled in the sixth step. 20 25
11. The payment method according to Claim 8 or 10, **characterized in that**, when the first program hash value and the second program hash value are encrypted in the third step, the encrypted first program hash value and the payment program are installed, as a coupled module, in the main board memory. 30
12. The payment method according to Claim 8, 10, or 11, **characterized in that** the first key to be used in the third step is an encrypted key produced by using the secret key and a random number, that the second key to be used in the fourth step is the encrypted key and public key, 35 40 45 50 55

FIG. 1

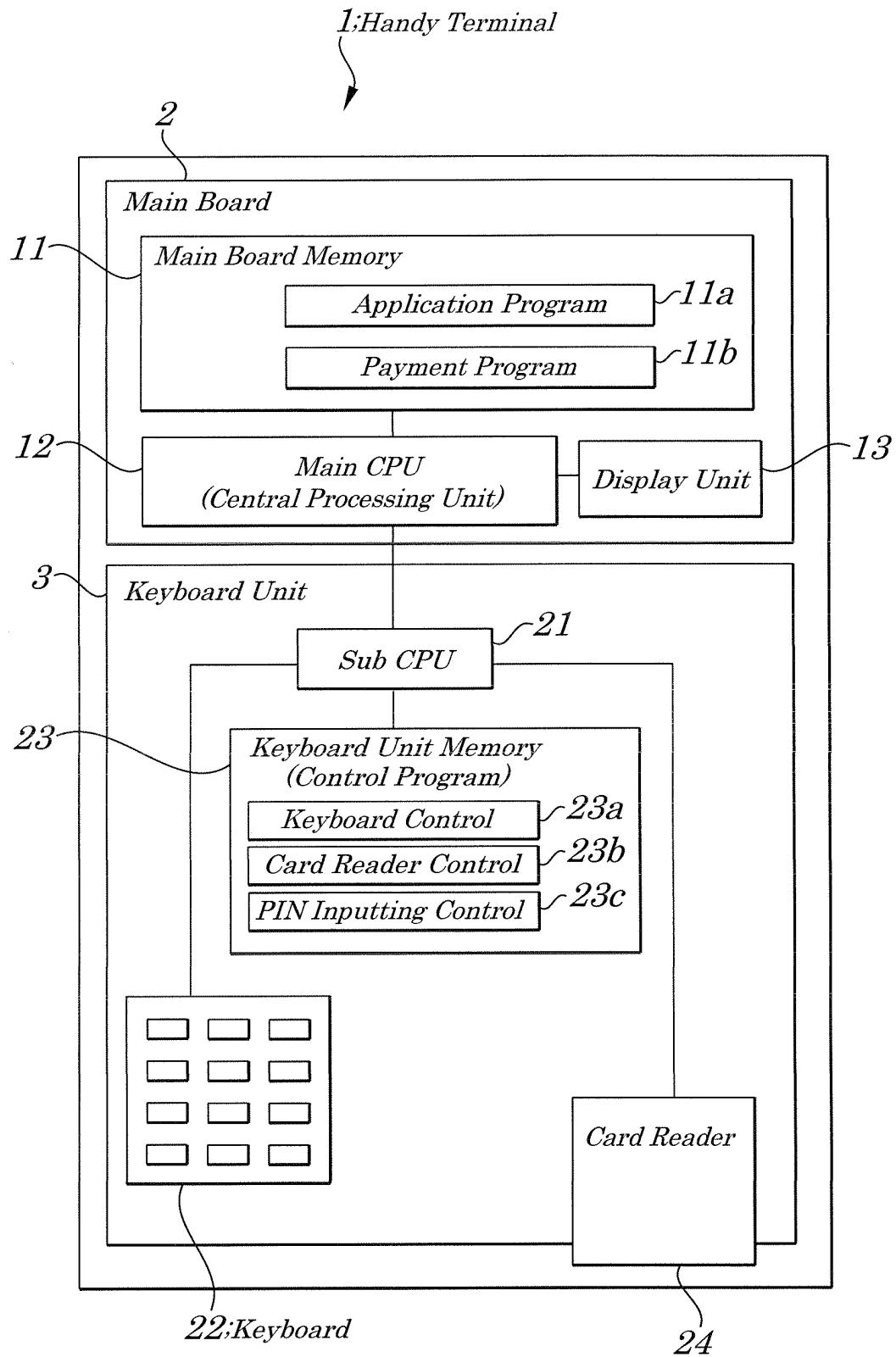


FIG. 2

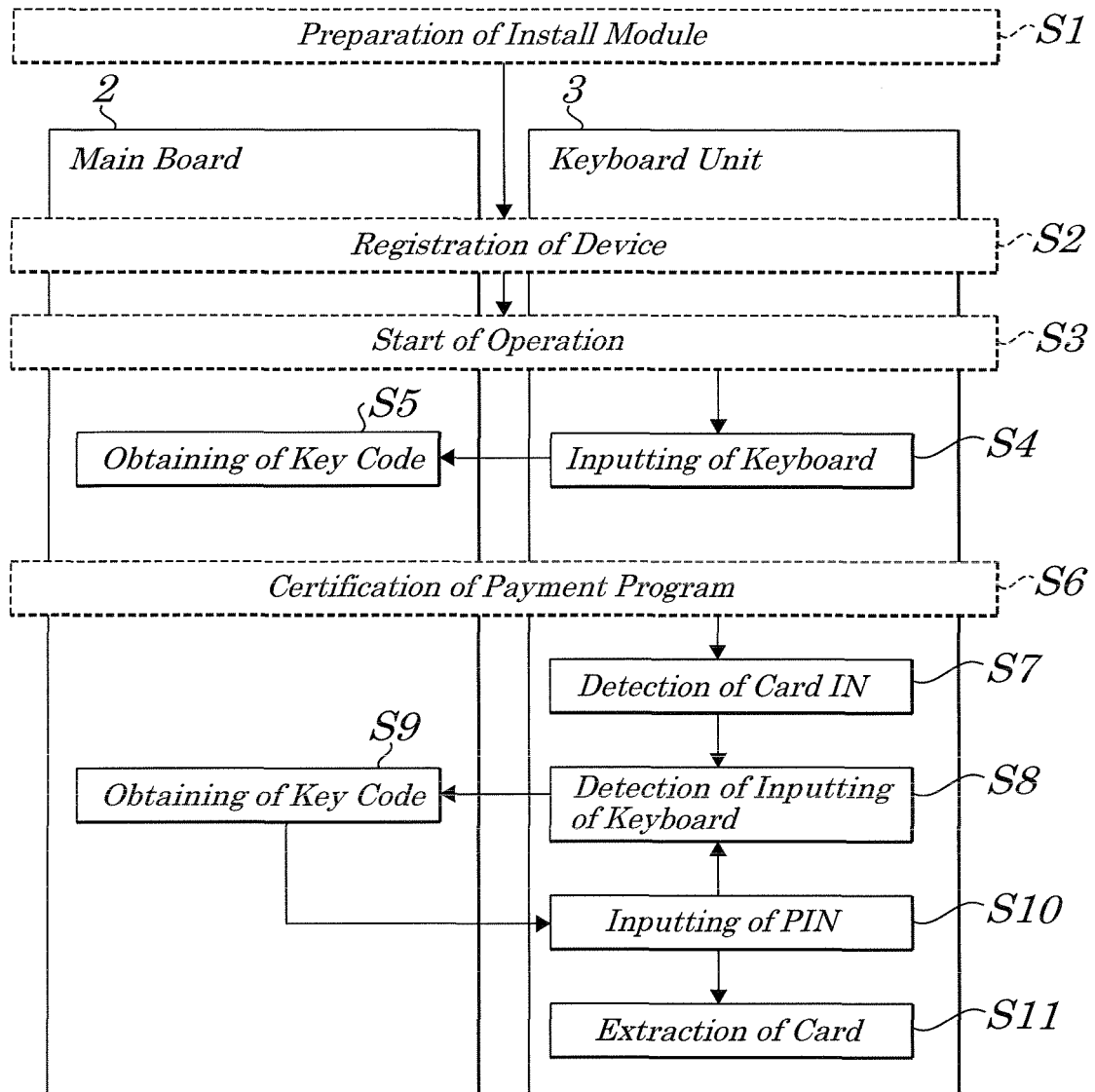


FIG.3

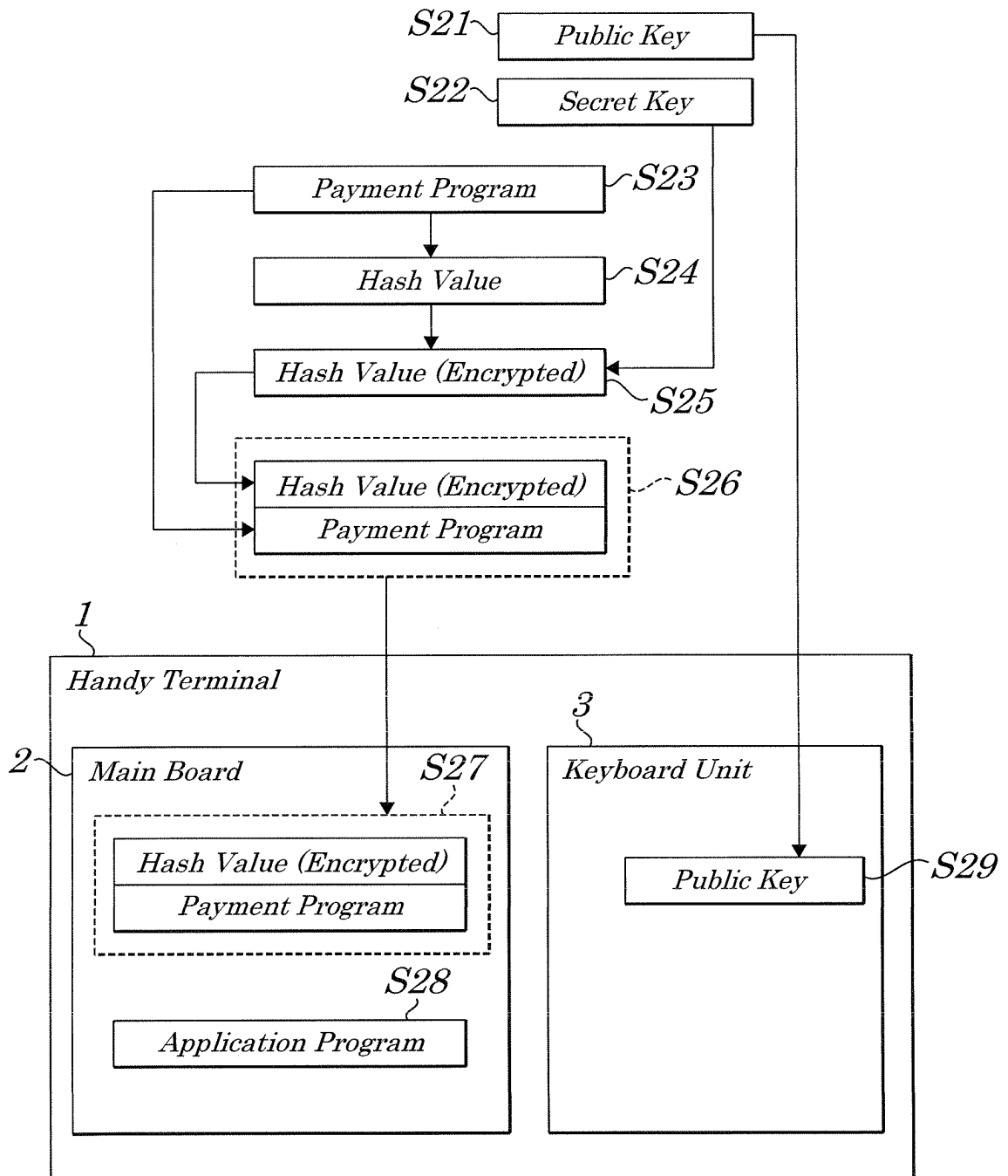
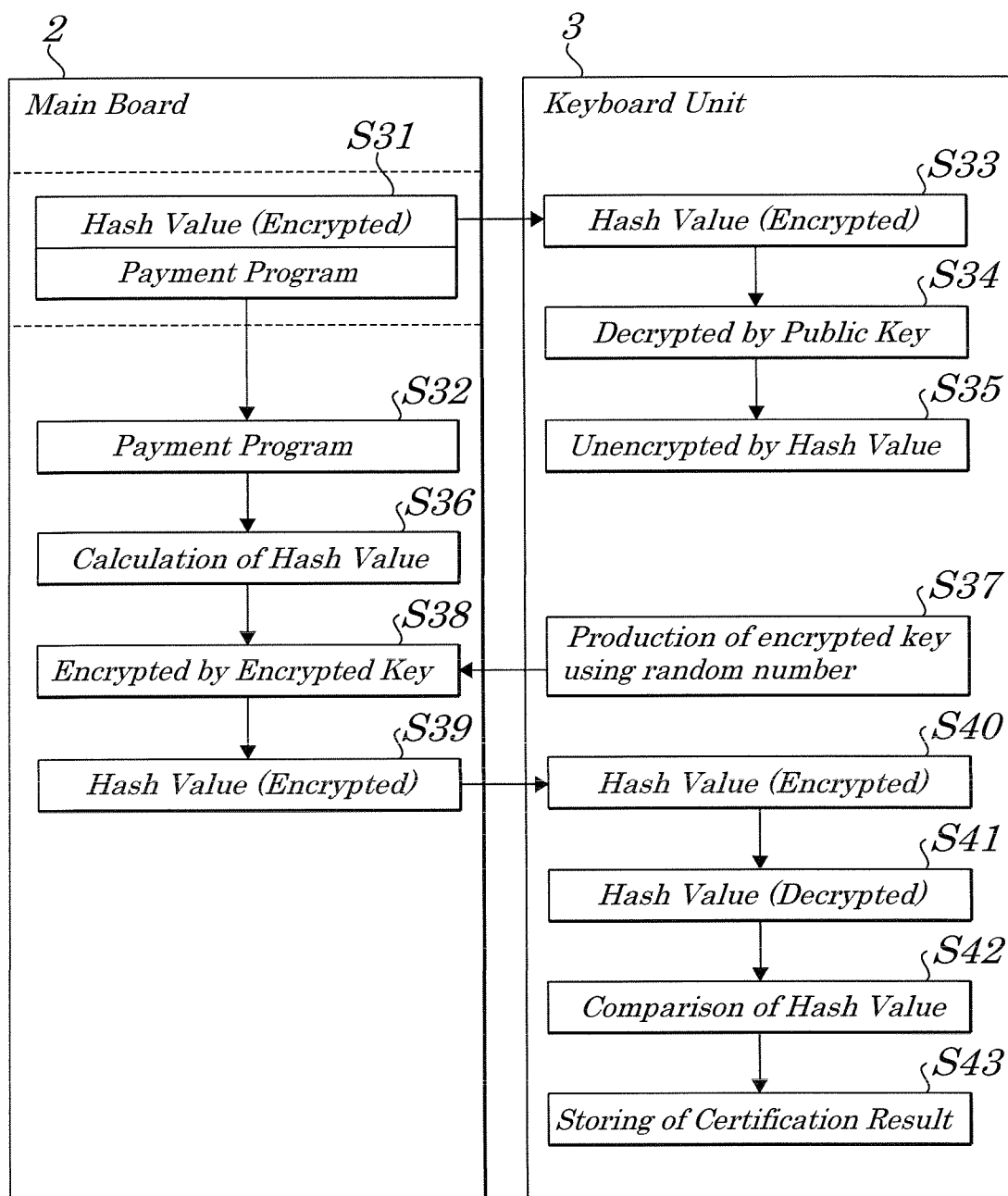


FIG. 4



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2010/069754

A. CLASSIFICATION OF SUBJECT MATTER <i>G07G1/12</i> (2006.01) i, <i>G06F21/20</i> (2006.01) i, <i>G06Q10/00</i> (2006.01) i, <i>G06Q20/00</i> (2006.01) i, <i>G09C1/00</i> (2006.01) i, <i>H04L9/32</i> (2006.01) i According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) <i>G07G1/12</i> , <i>G06F21/20</i> , <i>G06Q10/00</i> , <i>G06Q20/00</i> , <i>G09C1/00</i> , <i>H04L9/32</i> Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2010 Kokai Jitsuyo Shinan Koho 1971-2010 Toroku Jitsuyo Shinan Koho 1994-2010 Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2004/017255 A1 (Fujitsu Ltd., Fujitsu Frontech Ltd.), 26 February 2004 (26.02.2004), & US 2005/0145690 A1 & EP 1553518 A1	1-12
A	JP 2003-162758 A (NEC Corp.), 06 June 2003 (06.06.2003), (Family: none)	1-12
A	JP 2003-16527 A (Fujitsu Ltd.), 17 January 2003 (17.01.2003), & US 2003/0004877 A1 & EP 1271427 A3	1-12
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 29 November, 2010 (29.11.10)		Date of mailing of the international search report 07 December, 2010 (07.12.10)
Name and mailing address of the ISA/ Japanese Patent Office		Authorized officer
Facsimile No.		Telephone No.

Form PCT/ISA/210 (second sheet) (July 2009)

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- JP 2002133533 A [0006]
- JP 2005182315 A [0006]
- JP 2006178544 A [0006]
- JP 2009256218 A [0041]